

STATE OF NEVADA
DEPARTMENT OF HEALTH AND HUMAN SERVICES
DIVISION OF WELFARE AND SUPPORTIVE SERVICES
Information Systems
1470 College Parkway
Carson City, NV 89706
(775) 684-0500

DATE: 10-27-08

Corrected All Staff Memo #17

TO: All Staff

FROM: Nancy Ford, Administrator

SUBJECT: Secure E-mail

I am pleased to announce the introduction of secure e-mail. Beginning November 1, 2008, DWSS will be using a secure e-mail product that ensures the protection of personal information by using the leading identity-based encryption technology.

Attached you will find the *Introduction of Secure Email* document for your use and reference as you prepare to use secure e-mail. This document will also be posted on the Division's website.

INTRODUCTION OF SECURE E-MAIL

What is secure e-mail?

Secure e-mail ensures that personal information is protected and can only be read by the recipient by using the leading identity-based encryption technology. Secure e-mail is easy to use and enables you to receive, reply to, and initiate secure e-mail without the need to download or install any software.

Why does DWSS need secure e-mail?

Various state / federal laws and federal information exchange agreements require the use of encryption when transmitting personal information.

Nevada Revised Statute (NRS) 597.970 became effective on 10/01/08 and states,

“A business in this State shall not transfer any personal information of a customer through an electronic transmission other than a facsimile to a person outside of the secure system of the business unless the business uses encryption to ensure the security of electronic transmission.”

Is a state entity such as DWSS considered a business? What does secure system of business mean?

DWSS has requested the Department of Information Technology's (DoIT) Office of Information Security secure an interpretation of NRS 597.970 from the State Attorney General.

Unless the AG's opinion changes DWSS' interpretation, DWSS is considered a business and the secure system of business is considered to be within the State of Nevada, Department of Information Technology's (DoIT) e-mail system.

Is DWSS' Outlook e-mail system within the State of Nevada, DoIT's e-mail system?

Yes.

What entities e-mail systems are NOT within the State of Nevada, DoIT's e-mail system?

All Federal and/or County and some State entities are not part of the State of Nevada, DoIT's e-mail system. State entities that are not considered to be part of the State of Nevada, DoIT's e-mail system and have their own separate e-mail system are:

- Controller's Office
- Public Employees Benefits Program
- Department of Motor Vehicles
- Supreme Court
- Attorney General's Office
- Nevada Department of Transportation
- Department of Corrections
- Department of Public Safety
- Department of Employment Training and Rehabilitation

What is personal information?

NRS 603A.040 defines personal information (PI) as follows:

"Personal information means a natural person's first name or first initial and last name in combination with any one or more of the following data elements, when the name and data elements are not encrypted:

1. Social security number.
2. Driver's license number or identification card number.
3. Account number, credit card number or debit card number, in combination with any required security code, access code or password that would permit access to the person's financial account. The term does not include the last four digits of a social security number or publicly available information that is lawfully made available to the general public."

Secure e-mail provides e-mail usage reports for administration. What gives my employer the right to view my e-mail usage?

The State of Nevada Information Security State Standard 4.65 regarding e-mail became effective 01/11/02 and states,

"Employees shall be informed that all E-mail sent on state systems can be recorded and stored along with the source and destination. Employees have no right to privacy with regard to E-mail usage on state systems. Management has the right to view employees' usage patterns and take action to assure that agency Internet and E-mail resources are devoted to maintaining the highest level of productivity. Recorded E-mail messages from state systems are the property of the agency."

How does secure e-mail work?

When an e-mail is initiated or responded to by DWSS (identified by the extension dwss.nv.gov) secure e-mail will determine if the e-mail needs to be encrypted based on

predefined criteria. If it meets the predefined criteria the e-mail will be encrypted and sent to the recipient.

Do I have to have Cookies turned on?

Yes, Cookies must be enabled in order to access secure e-mail.

Will secure e-mail distinguish between a Social Security Number (SSN) and a Unique Person Identifier (UPI)?

No. As a result, secure e-mail will encrypt both.

Will secure e-mail distinguish between a pseudo SSN and an actual SSN?

No. As a result, secure e-mail will encrypt the message.

Will secure e-mail scan for PI captured within a snap shot or screen shot?

Example: A snap shot of a NOMADS production screen with client PI is pasted into a Word document and attached to an e-mail or is pasted directly into the body of an e-mail.

No. Secure e-mail only scans text and views a screen shot or snap shot as a graphic. Screen shots or snap shots that contain PI should be sent as a password protected attachment.

When will secure e-mail begin?

November 1, 2008. Each Friday between the initial introduction and 11/1/08, this secure e-mail communications document will be sent via e-mail to all known entities, with daily e-mail announcements occurring 10/27/08 through 10/31/08.

As an external entity with the ability to support Transport Layer Security (TLS), can we choose to use TLS so this secure e-mail implementation will have zero impact to our e-mail users?

Yes, we highly encourage the use of TLS for those external entities that routinely receive DWSS e-mail that may contain PI. Please have your technical support staff contact the DWSS Operations Manager to initiate the use of TLS:

Bart London
775-684-0591 Office
775-691-2963 Cell
Blondon@dwss.nv.gov

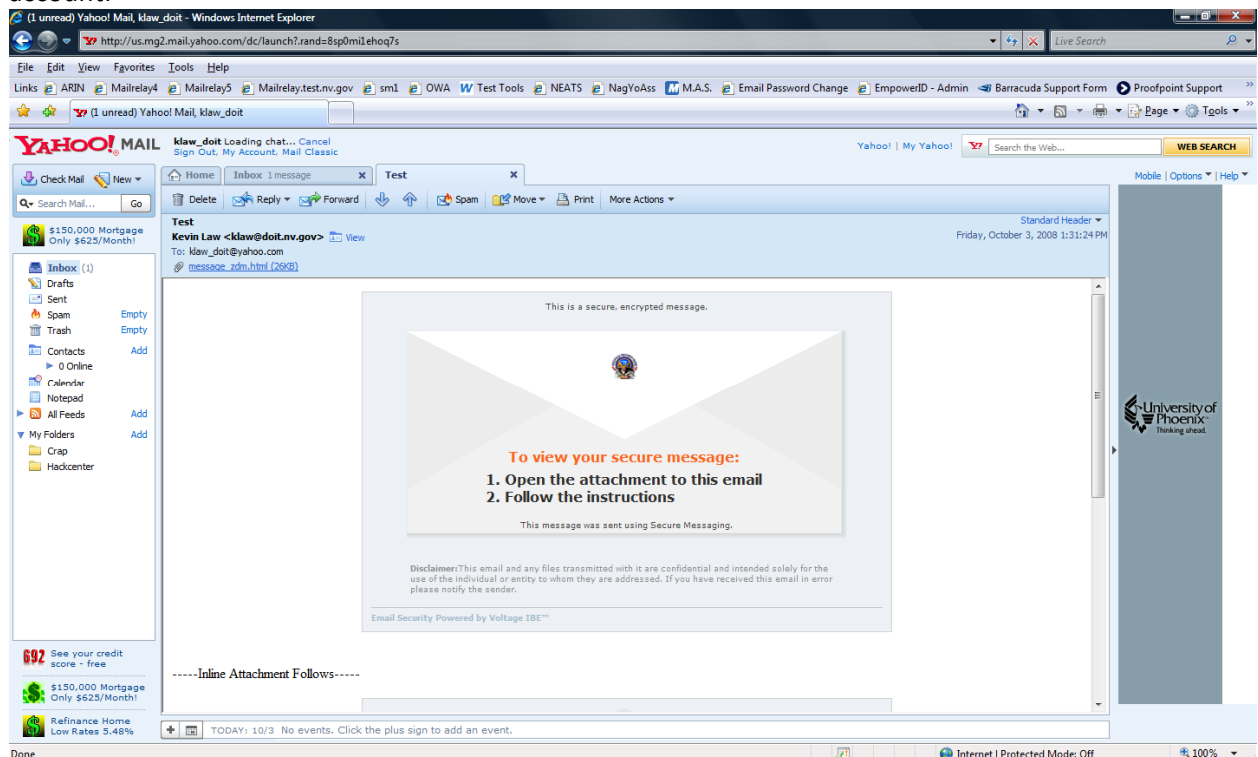
Do external entities have to support TLS to read a secure e-mail?

No.

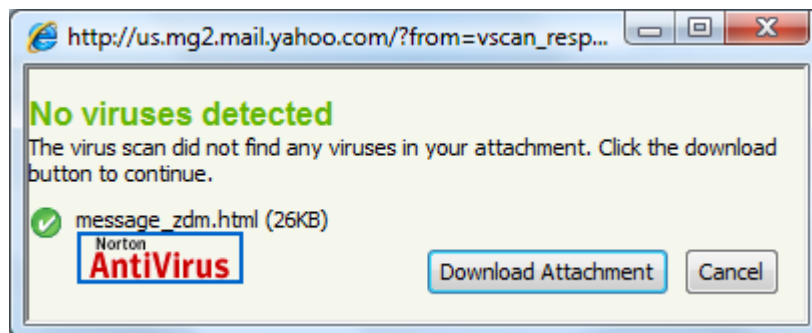
How do I as the recipient read a secure e-mail?

The end user presentation may differ pending on which web browser is being used by the recipient. This document uses both Yahoo and Charter to illustrate the end user presentation.

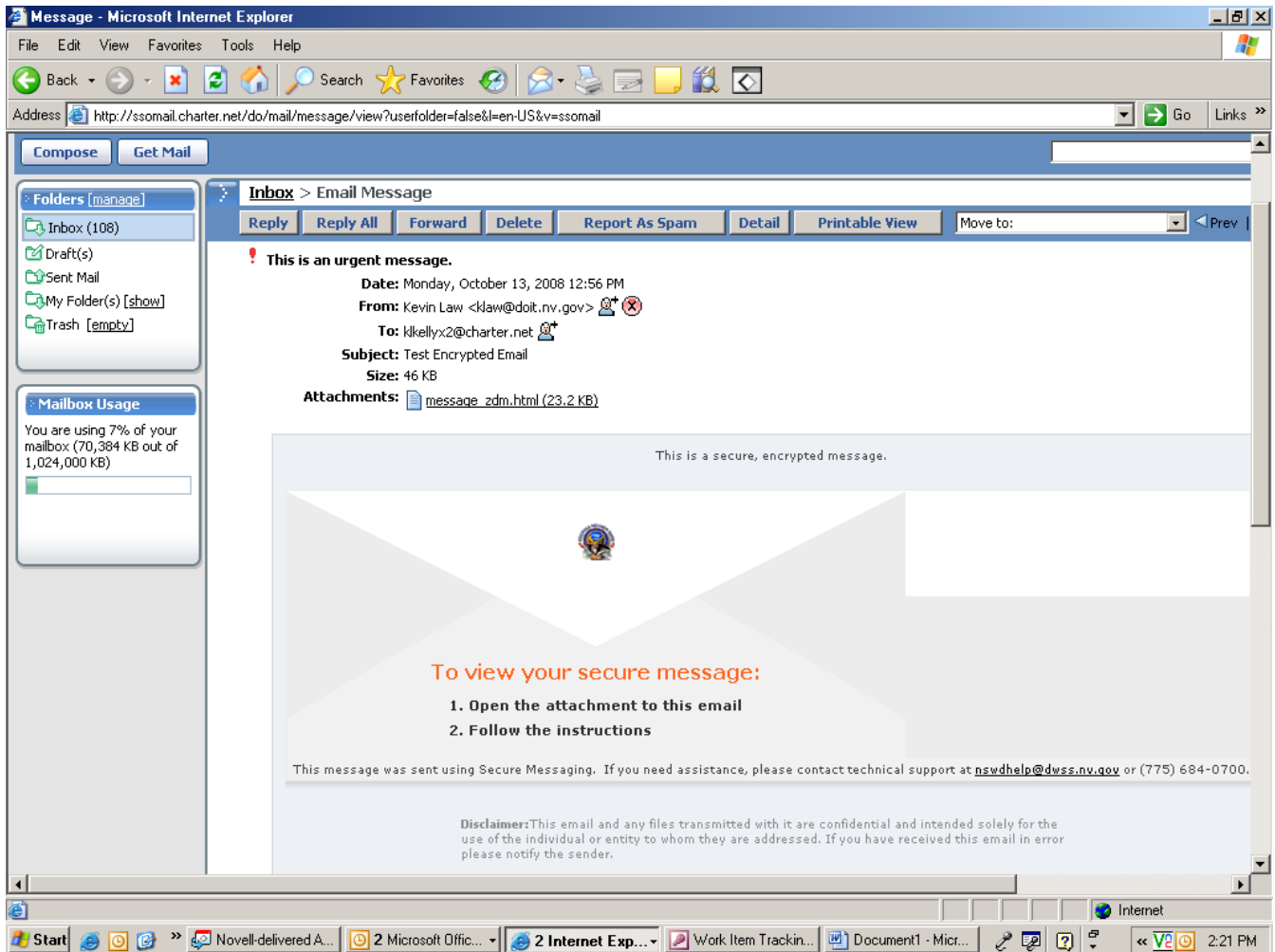
Here is what a secure e-mail looks like when it appears in the “inbox” for a Yahoo webmail account:



When following the instructions to open the message and clicking on the attachment, Yahoo webmail does an antivirus scan on the attachment.

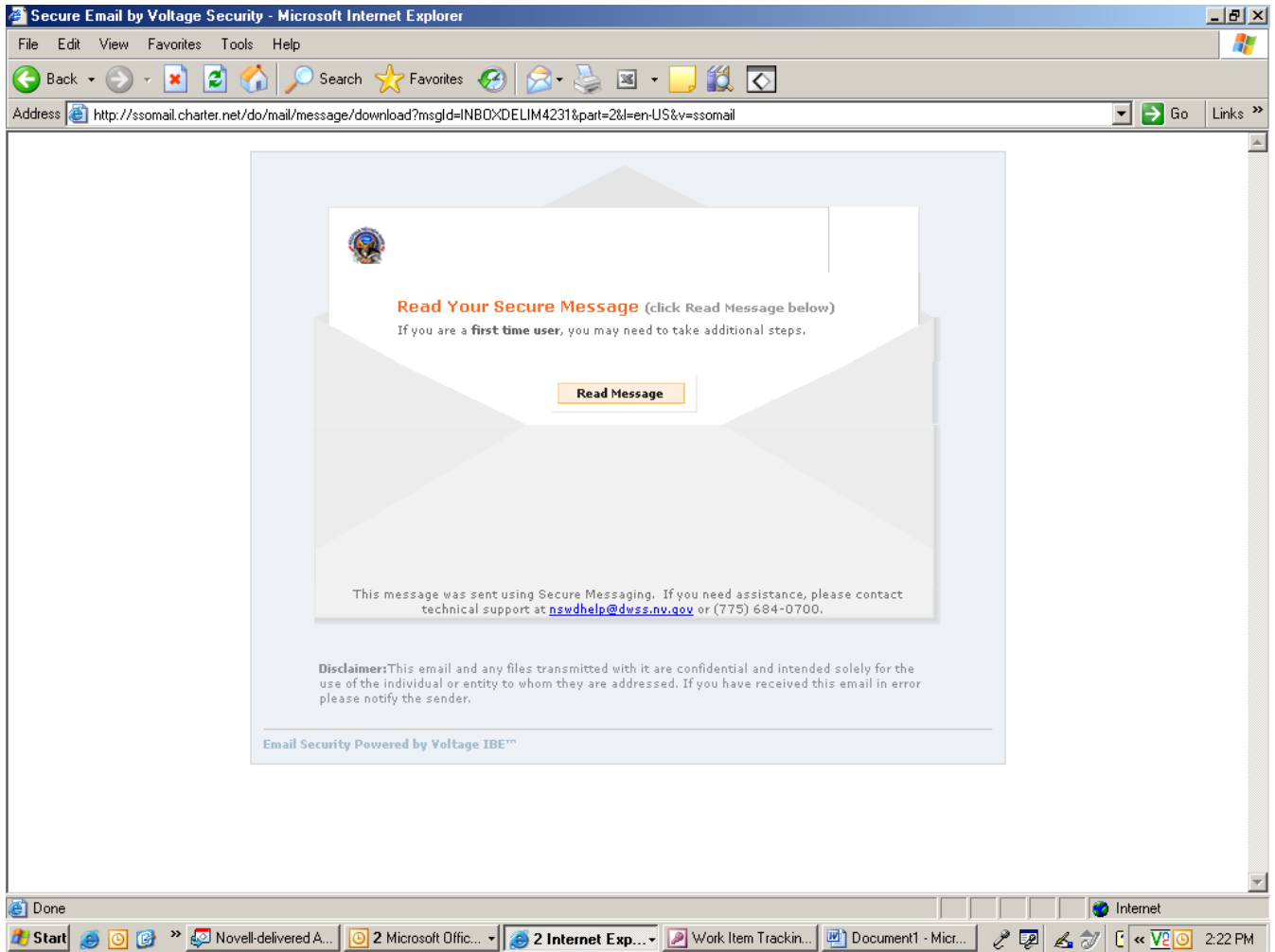


Here is what a secure e-mail looks like when it appears in the “inbox” for a Charter webmail account:



The secure e-mail recipient must click on the “message_zdm.html” attachment.

After the attachment is opened the secure e-mail recipient will see the following “Read Your Secure Message” and must click on the “Read Message” button.



The first time a secure e-mail recipient attempts to read a secure e-mail they will need to create a SecureMail ID.

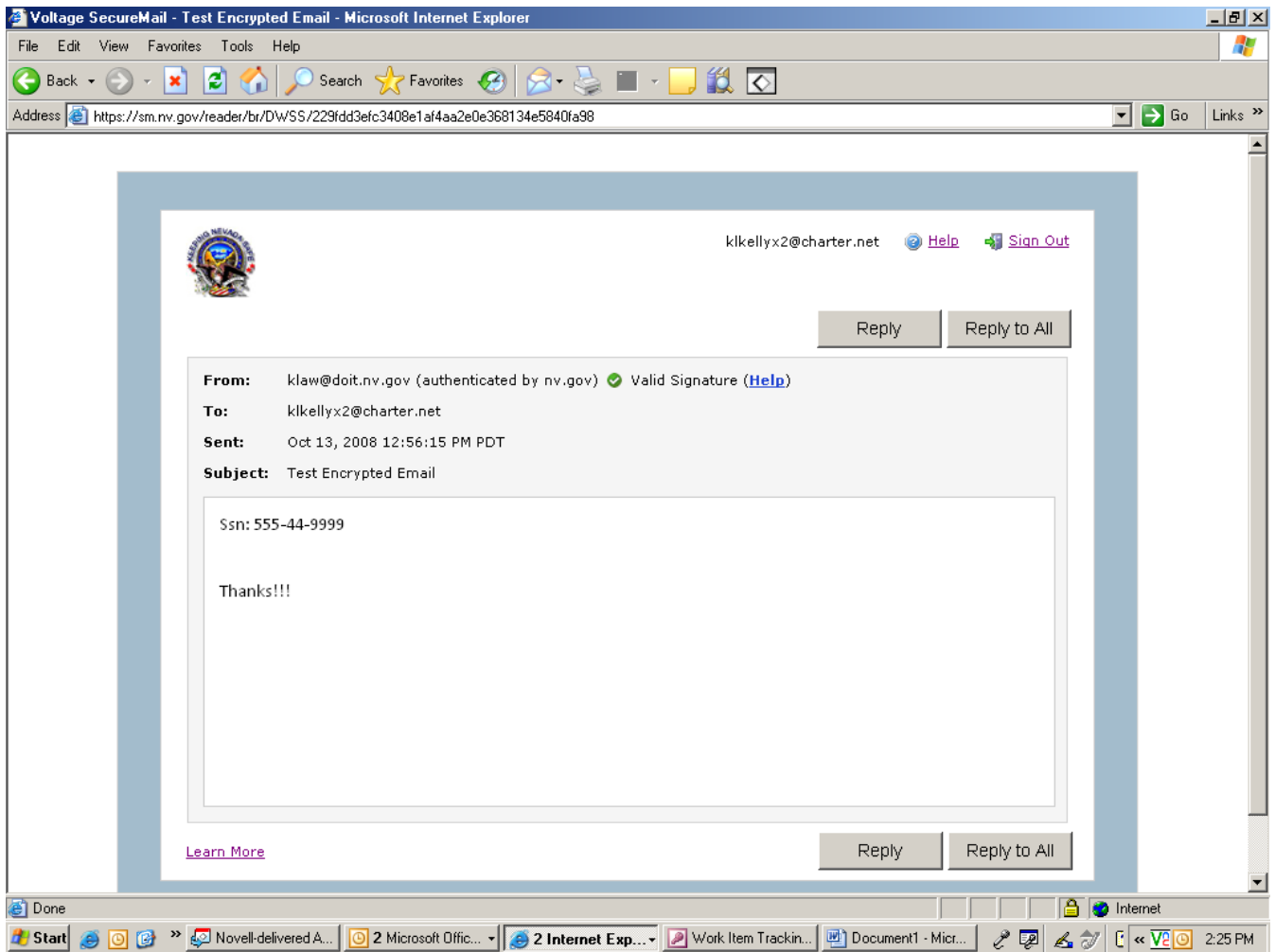
The screenshot shows a web browser window titled "Voltage SecureMail - Zero Download Messenger - Microsoft Internet Explorer". The address bar displays a long URL starting with "https://sm.nv.gov/es?key=MFwwDAYKYIZIAYb9HglBAQwRbnYuzZ292IzEyMTczNjUwNTIwOTAaDAIub3RCZWZvcmlUEDTA4MTAxMTAwMDAwMFowGwwCaWQEFWtsa". The main content area features a "Create Your SecureMail ID" form with the following fields:

- Name:
- Email Address: **klkellyx2@charter.net**
- Password:
- Verify Password:
- Recovery Question: **Please choose one** (dropdown menu)
- Answer:

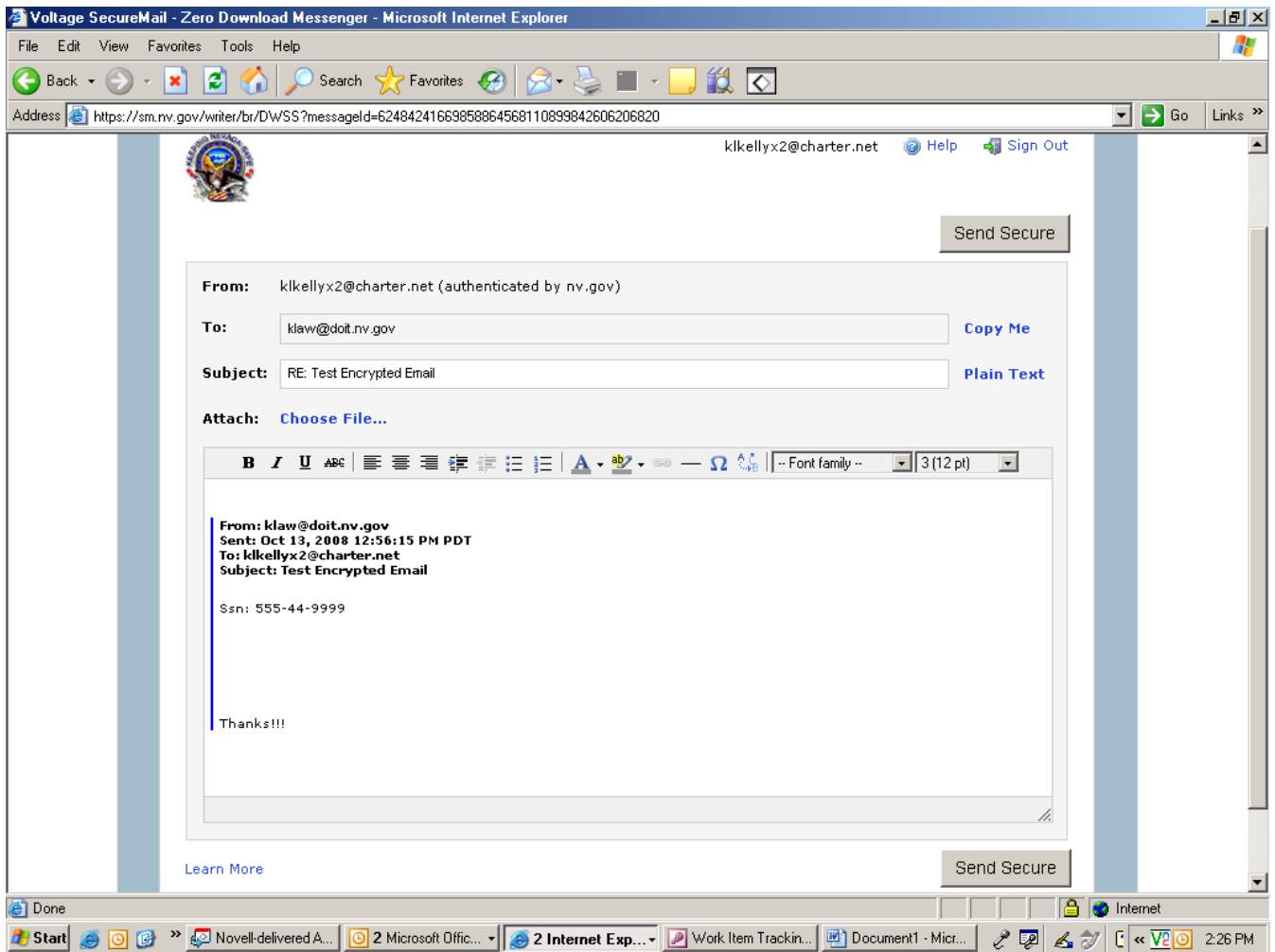
A "Continue" button is located at the bottom right of the form. Below the form, a privacy notice states: "We value your right to privacy. We will never use your email address to send you unsolicited mail, and we will never share it with or sell it to a third party. If you need assistance, please contact technical support at nswdhelp@dwss.nv.gov or (775) 684-0700."

The Windows taskbar at the bottom shows the Start button, several open applications including "Novell-delivered A...", "2 Microsoft Offic...", "2 Internet Exp...", "Work Item Trackin...", and "Document1 - Micr...", and a system clock showing "2:22 PM".

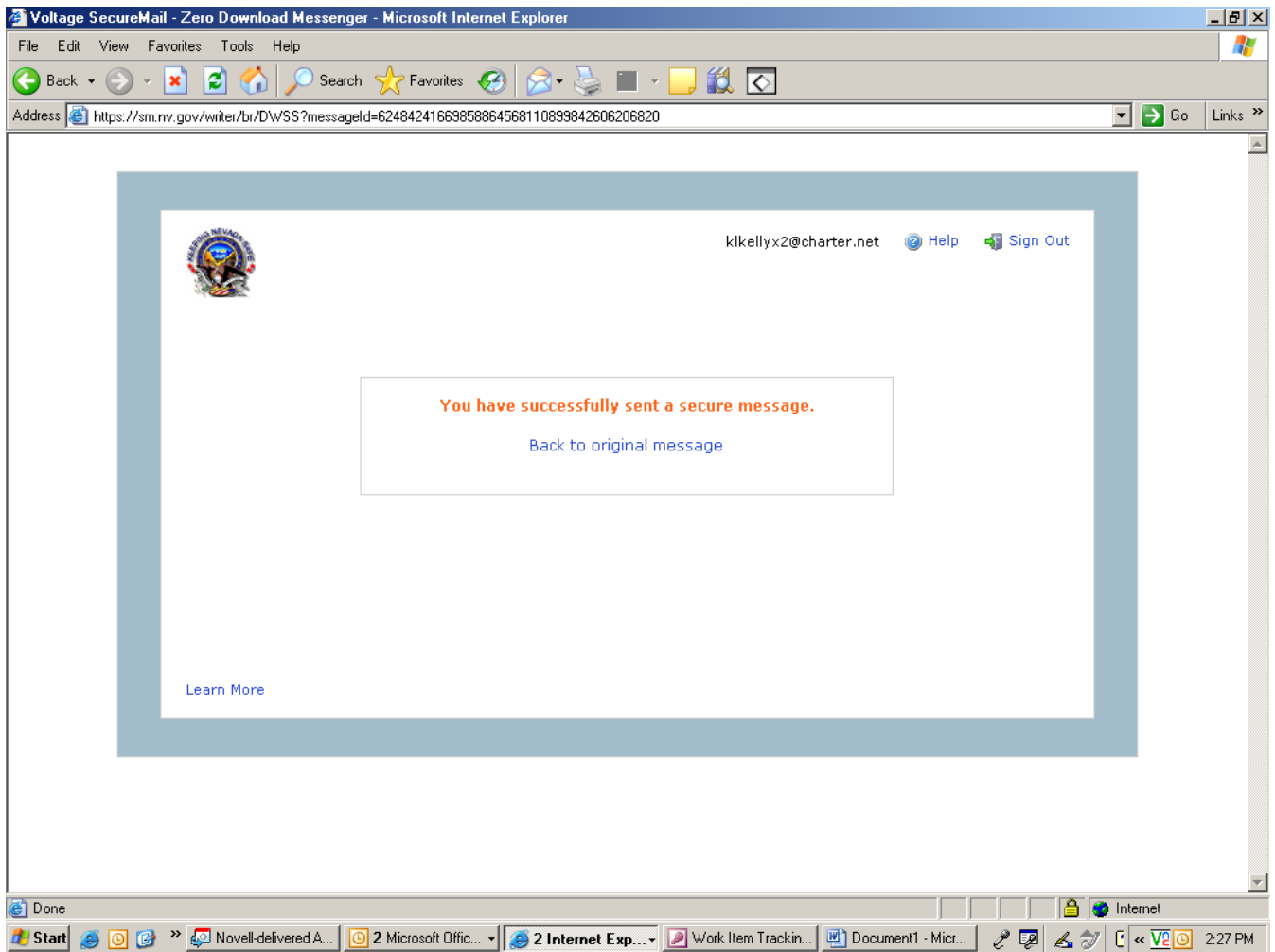
The secure e-mail recipient enters the following information: Name; Password; Verify Password; Selects the Recovery Question; and provides the response, clicking on CONTINUE will present the secure e-mail message:



When the secure e-mail recipient clicks Reply or Reply to All they will see:



After clicking the SEND SECURE button the following displays:



Who do I contact if I have a problem opening a DWSS.nv.gov secure e-mail?

If you need assistance, please contact technical support at nswdhelp@dwss.nv.gov or call (775) 684-0700.

The secure e-mail help tool has valuable information and can be used at any point by clicking on HELP.

The following information has been copied from the secure e-mail help tool to provide additional information:



Using Secure Messaging

Contents:

- [Receiving Secure E-mail](#)
- [Replying to Secure E-mail](#)
- [Forwarding Secure E-mail](#)
- [Initiating Secure E-mail](#)
- [Using Zero Download Messenger Rich Content](#)
- [Security](#)

Receiving Secure E-mail

How do I read a secure e-mail?


To read your secure e-mail, click the "message_zdm.html" attachment. Next, click the "Read Message" button on the page that opens in your web browser.

To complete the process, you will be asked to authenticate yourself in the manner designated by the company you are communicating with. When the authentication process completes, the secure e-mail will be displayed in your web browser.


How do I access attachments sent to me?

All secure attachments are contained within a single Zero Download Messenger package to enable easy access. To open the attached files, click on the [view] button next to the attachment names - a new browser window will open to enable you to access the attachment.

What are signatures and what does it mean if the signature is valid with ?

Every secure e-mail is signed by the sender of the message to ensure authenticity of the sender and data integrity of the message. The  indicates that the signature associated with this e-mail is valid and the message can be trusted.

What are signatures and what does it mean if the signature is invalid with ?

Every secure e-mail message is signed by the sender of the message to ensure authenticity of the sender and data integrity of the message. The  means that the signature associated with this message is not valid and the message may have been forged. We recommend that you either contact the sender of the message or technical support at nswdhelp@dwss.nv.gov or (775) 684-0700.

Replying to Secure E-mail

How do I reply to a secure e-mail?

If permitted by the company you are communicating securely with, you can have the option to reply back to the received secure e-mail. To do so:

- Click the "Reply" button located at the top of the message to reply only to the sender of the message. If you would like to reply to everyone, click on "Reply All" button instead. This will send your reply to all recipients of the original message, as well as the sender of the message.
- Next, a compose window will appear. If you clicked "Reply," only the sender's e-mail address will appear in the To: field.
- If you clicked "Reply All", the sender's and recipients' addresses will appear in the To: field. If desired, you may also add new e-mail addresses. Additional e-mail address can be separated with commas, semi-colons or blank spaces
- Type your reply. The original message is already included in the compose field - you can type in the area above, below or within the sender's message.
- Click "Send Secure" to send your reply.

How do I add an attachment to the secure e-mail?

If permitted by the company you are communicating securely with, you can have the option to add an attachment to your e-mail.

You can send all types of files as attachments, including word processor or spreadsheet documents, audio files, image files (.bmp, .jpg, .gif, etc.), web pages saved as HTML files, and more.

The compose page will display the maximum total attachment size permitted next to the Total Attachment Size field. The maximum number of attachments allowed on each secure e-mail is designated next to the Maximum Allowed Attachments field.

To add attachments to your secure e-mail:

- Click the "Browse..." button located at the end of the Attach File field
- When you have selected a file, click the "Attach" button located next to the "Browse..." button
- Once the file has been uploaded, the compose page will be updated with the name of the file displayed underneath the Attach Field field. A remove link is provided to allow you to remove an attachment.
- To add additional attachments, repeat steps (a) and (b)

How do I get a copy of the secure e-mail that I have composed?

You may get a copy of the secure e-mail that you have composed sent back to your e-mail address. By default, this is enabled by the checked box next to the "Send Me a Copy" field. When you click on the "Send Secure" button, an exact same copy of the composed secure e-mail is sent to your e-mail account. If you do not want to have a copy of the secure e-mail, you may uncheck the box.

Forwarding Secure E-mail

How do I forward a secure e-mail?

If permitted by the company you are communicating securely with, you can have the option to forward the received secure e-mail to new recipients. To do so:

- Click the "Forward" button located at the top of the message to forward the message
- Next, a compose window will appear. E-mail addresses can be added into the To: field and separated with commas, semi-colons or blank spaces
- If you like, you may include an additional message to the original e-mail that is included in the compose field - you can type in the area above, below or within the original message.
- Received attachments will be included in the forwarded e-mail message body
- Click "Send Secure" to send your forward.

Initiating Secure E-mail

How do I initiate a secure e-mail?

If permitted by the company you are communicating securely with, you can have the option to initiate a secure e-mail through a provided webpage link. To do so:

- Go the provided webpage to create your secure e-mail
- Sign in by entering your e-mail address and click "Next"
- At this point, you will be asked to authenticate yourself in the required manner designated by the company you are communicating with.
- Upon completion of the authentication process, a compose page will be displayed.
- E-mail addresses can be added into the To: field and separated with commas, semi-colons or blank spaces
- Enter the subject of your message in the Subject: field.
- Compose your message in the large text box
- To attach a file to your secure e-mail, click on "Browse..." to select a file from your desktop. Click "Attach" to complete the process.
- Once you have completed the above steps, click on the "Send Secure" button to send the message.

Enabling Cookies in Your Web Browser

Contents:

- [Windows Internet Explorer](#)
- [Firefox](#)

Windows Internet Explorer

1. Under the Tools menu, select "Internet Options".
2. In the Internet Options window, select the "Privacy" tab.
3. Click the "Advanced" button.
4. Check the box to "Override automatic cookie handling".
5. In Advanced Privacy Settings window, for First-party Cookies, select "Accept".
6. Click the "OK" button on the Advanced Privacy Settings window.
7. Click the "OK" button on the Internet Options window.

Firefox

1. Under the Tools menu, select "Options".
2. In the Options window, select "Privacy".
3. In the Cookies section, ensure that the box next to "Accept cookies from sites" is checked.
4. Click the "OK" button.

Using Zero Download Messenger Rich Content

There is a known conflict between ZDM Rich Content and Internet Explorer 6 Content Advisor. In order to successfully compose ZDM messages, please temporarily disable IE Content Advisor.

- From within Internet Explorer 6, select Tools --> Internet Options
- Select Content
- Click Disable under Content Advisor
- Provide the password you set when Content Advisor was enabled

Security

How secure is the Zero Download Messenger?

The Zero Download Messenger secure e-mail is encrypted with the equivalence of a 1024-bit key. It uses the breakthrough Identity-Based Encryption to ensure the privacy of your personal data without compromising on ease of use. Each message is also signed by the sender to ensure authenticity of the sender and data integrity of the message.

About Secure E-mail and Identity Based Encryption (IBE)

Contents:

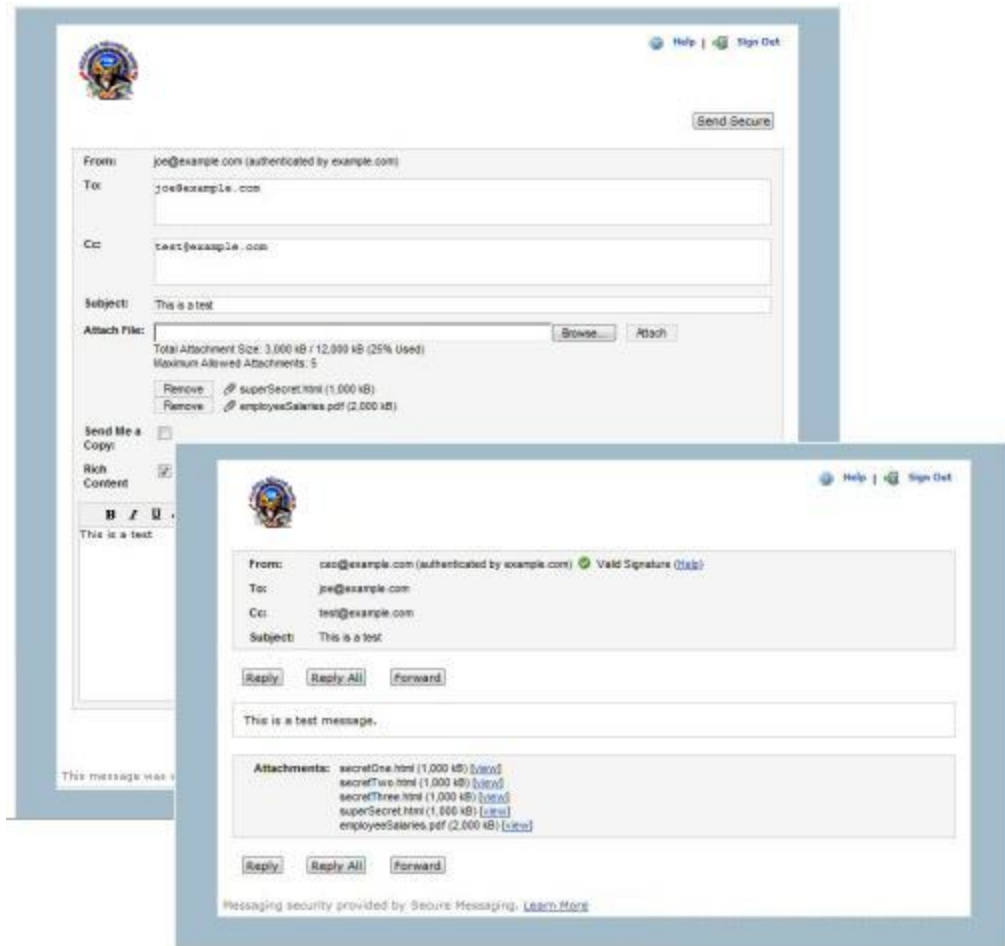
- [About Secure E-mail](#)
- [What is Identity Based Encryption \(IBE\)?](#)

About Secure E-mail

Voltage Secure-mail enables usable secure e-mail. With Voltage Secure-mail, communication of sensitive information remains private and secure, enabling companies to meet compliance requirements such as Gramm-Leach-Bliley Act (GLBA), FFIEC Bank Examinations, Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley, 21 CFR Part 11 and California SB 1386. To provide proof of compliance during an audit, Voltage Secure-mail also maintains complete audit trails for each Voltage Secure-mail user, including logs of when messages were opened.

What is secure e-mail?

Secure Messaging ensures that your sensitive information is protected and can only be read by you. Your secure e-mail has been encrypted with the leading Identity-Based Encryption technology. Secure Messaging makes secure e-mail easy to use and the Zero Download Messenger enables you to receive, reply to, and initiate secure e-mail without the need to download or install any software.



What is Identity Based Encryption (IBE)?

Secure Messaging uses a breakthrough approach in cryptography known as Identity-Based Encryption (IBE). IBE enables a simple identity, such as an e-mail address, to be used as public key to facilitate secure communication with any recipient. IBE does not require end-user certificates and thereby eliminates the usability and management problems inherent in traditional PKI based communication solutions.